CLAIMS

1. A cryptographic method during which an integer division of the type q = a div b and/or a modular reduction of the type r = a mod b is performed, with q a quotient, a a number of m bits, b a number of n bits, n less than or equal to m and b_{n-1} non zero, b_{n-1} being the most significant bit of the number b, characterised in that the number a is masked by a random number ρ before performing the integer division and/or the modular reduction.

2. A method according to Claim 1, during which, in order to mask the number a, b times the random number ρ (a <- a + b*ρ) is added to the number a.

3. A method according to Claim 1 or Claim 2 in which, after having performed an integer division, the contribution made by the random number ρ is taken away from the result of the integer division.

4. A method according to Claim 3 in combination with Claim 2, during which, in order to take away the contribution made by the random number ρ, the said random number ρ is subtracted from the result of the integer division.

5. A method according to one of Claims 1 to 4, during which the random number ρ is modified at each implementation of the method.

6. A method according to one of Claims 1 to 4, during which the random number ρ is modified after a predetermined number of implementations of the method.

7. An electronic component comprising means for

implementing a method according to one of the preceding claims, the programmed calculation means comprising in particular several registers for storing the numbers a and b.

8. A chip card comprising a component according to the preceding claim.